IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

_____

DONNA CURLING, ET AL.,

Plaintiffs,

vs.

BRAD RAFFENSPERGER, ET AL.,

Defendants.

_____

CIVIL ACTION FILE
NO. 1:17-CV-2989-AT

VIDEO-RECORDED 30(b)(6) DEPOSITION
TAKEN VIA VIDEOCONFERENCE OF
GEORGIA SECRETARY OF STATES' OFFICE
BY: SANFORD MERRITT BEAVER
AND
SANFORD MERRITT BEAVER
IN HIS PERSONAL CAPACITY
(Taken by Plaintiffs)
Atlanta, Georgia
Wednesday, February 2, 2022
9:08 a.m.

Reported stenographically by
V. Dario Stanziola, CCR (GA)(NJ), RPR, CRR

INDEX OF EXAMINATIONS

INDEX OF EXHIBITS

THE VIDEOGRAPHER: We are on the record February 2nd, 2022 at approximately 9:08 a.m. Eastern time. This will be volume II to the 30(b)(6) videotaped deposition of the Secretary of State's office. The representative today will be Merritt Beaver. Will counsel please identify themselves and who they represent for the record.

MR. CROSS: This is David Cross of Morrison & Foerster for the Curling plaintiffs.

MR. DENTON: This is Alexander Denton of Robbins Alloy Belinfante Littlefield for the state defendants.

THE VIDEOGRAPHER: Will the court reporter please swear in the witness.

(OATH ADMINISTERED.)

SANFORD MERRITT BEAVER,

having first been duly sworn, was examined and testified as follows:

EXAMINATION

BY MR. CROSS:

Q. Good morning, Mr. Beaver.

Are we picking you up okay?

Q. Have you been deposed before?
Sorry, did you say yes?
Yeah, we're not getting that.
Yeah, let's go off the record. Your mic's not working.
THE VIDEOGRAPHER: The time is 9:11. We're off the record.
(A DISCUSSION WAS HELD OFF THE RECORD.)
THE VIDEOGRAPHER: The time is 9:13. We're back on the record.
BY MR. CROSS:
Q. All right. Good morning, Mr. Beaver. We'll try this again.
A. Good morning again.
Q. And I think you said you have or have not been deposed before?
A. I have been deposed before.
Q. Okay. All right. And did you meet with counsel before your deposition today?
A. Yes.
Q. Okay. So do you understand that you're testifying today not just in your personal capacity, but as a representative of the Secretary of State's office on particular topics?
A. Yes, I do.

Q. And do you understand that means that you're testifying as to the knowledge and information that the Secretary's has on those topics?

A. Yes, I do.

Q. Okay. So do you have exhibit share up in front of you?

A. No. I need to click on something?

Q. Oh.

MR. CROSS: Let's go off the record again.

THE VIDEOGRAPHER: The time is 9:14 We're off the record.

(A DISCUSSION WAS HELD OFF THE RECORD.)

THE VIDEOGRAPHER: The time is 9:17. We're back on the record.

(Exhibit 1: Curling Plaintiffs' Second Amended Notice of Deposition of Office of the Secretary of State marked for identification, as of this date.)

BY MR. CROSS:

Q. Mr. Beaver, do you have Exhibit 1 in front of you?

A. I do.

Q. Have you seen this document before?

there was malware on it, if it at any way managed to get to a new platform, it would be inert, meaning it would have no capabilities in the new environment. Because based on this question, the malware was targeting the old election system, which was Windows-based using access database application.

One of the smartest things that the Georgia Secretary of State did was we moved to a system that was completely different, meaning it didn't use the same operating system, did not use the application prior used, which means that anything that was targeting that system would be inert in a new system. But even knowing that, we did make sure that it didn't exist.

Q. Okay. Let me -- we'll come back to that answer. But let me come back to the question I asked you. What did you do to prepare to testify on topic 1A?

A. I validated with my team that we built out a whole different system not connected at any reason or physically or electronically to the old system. We had no components of the old system, no software, no data, no anything. And the reason was the two systems were so different

there was absolutely nothing in the old system that was useful in the new system. So there was no reason to move any of that stuff over there. The old system was old equipment. We didn't need to use any old equipment. We started fresh. And there was nothing on the old system that was needed in the new system. So there was no effort to even try to connect the two. Because it would have made no value, added no value.

Q. When you say you validated this with your team what did you do to validate that?

A. I met with my team, met with the people that were actually hands on doing it, the work, and validated this is the process we follow.

Q. When did you do that?

A. Probably at least two or three weeks ago. Well -- and I -- we did it a long time ago when we actually did the move. We met and talked about how we were going to do it. That was back when we actually built out the new system. We did a whole plan as to how we would built -- would build it out. There was conversation of is there anything needed from the old system? The answer was no. Do we need any of the data on the system? No. So there was no effort to even try

to do anything with the old system. When we finished using the old system we just turned it off.

Q. When did that happen?

A. We walked away from it.

Q. When did that happen?

When did you turn off the old system?

A. It was -- I'd have to go back and look. I mean, I'd be guessing right now.

Q. Do you have any time frame?

Was it 2019 when you rolled out the new system or was it 2020?

A. We had the old system still on -- I'll say turned on. But we essentially -- we call it put it over in the corner because nobody was using it for about six months just in case there was any questions about something that was done in that system. So it would be somewhere towards the end of '19, probably into early 2000 that we literally unplugged it.

Q. And did servers from the old system sit in the same environment as the new system at any point?

A. Nope. They were in totally different racks. In fact, the rack was on wheels. When we

finished we literally rolled it into a caged area that was locked, pulled all the cables off of it and left it in a secure area. So it -- nobody could accidentally get into it. It would have taken somebody from my group to go reset it up.

Q. Okay. Who did you meet with you said about two or three weeks ago to validate this for the system?

A. Who did I meet with? My director of technology. My -- a couple of the people that work with him.

Q. What's his name?

A. Jason Matthews.

Q. You said Jason Matthews?

A. Yeah, Jason Matthews.

Q. And who else did you meet with?

What are their names?

A. Ronnell Spearman and Kevin Fitts.

Q. And they are report to the director of technology?

A. Yes.

Q. And were they the ones that were responsible for setting up the -- the new system and turning off the old one?

A. Ronnell was involved in that group,

were brand new. We started clean, fresh. We did not take any chances by introducing anything old.

Q. And how do you -- I'm sorry. Go ahead.

A. We did not share any of the networking infrastructure. That was all new.

Q. And are you saying -- you're also saying that there is no data in the old system that's used with the new system?

A. Correct. As I said, it's not compatible.

Q. So how does that work for the data in E-Net? Doesn't --

A. So -- so for the new system, we had to go back to E-Net and get new data and bring it over to the new system.

Q. All right. So how did you do that?

I thought you said there's no data from the old system used in the new system?

A. The old system -- there are multiple systems. Their E-Net is not the voter -- the votering balloting system. The question that this test talks about is all of the ballot and voting system, not the voter registration system. So when you're speaking of the system, I need you to tell me which system you're talking about. So

voter registration system is different than the ballot generation system that feeds the -- the vote-taking system, the voting system. It's two complete environments. Two totally different systems.

Q. So you don't --

A. The only thing that comes from one to the other is E-Net will export information about candidates over to the balloting system.

Q. Do you not consider Georgia's voter registration system part of the state's election system?

A. That is an umbrella statement. And when you say the election system, there are numerous systems. They're not tied together. They're all independent systems that are run and managed independently. So you can't apply something about one system to the other system. Operating systems are different, applications are different. The actual users are different.

Q. So let me -- let me just make sure I understand. I just want to see -- so does Georgia's election system include the voter registration database or that's something separate?

Q. Okay. So answer to my question is yes, the election system includes the voter registration database; are we agreed on that or not?

MR. DENTON: Objection.

A. The election system is a umbrella which I consider covers many systems where the voter registration system is one of those systems under what we call the elections system.

(Exhibit 2: Declaration of Merritt Beaver marked for identification, as of this date.)

Q. All right. Mr. Beaver, grab Exhibit 2. We'll come back to Exhibit 1. So you may want to leave that up, if you can.

A. Is that -- is there something new in here that I've got to look at?

Q. Yeah. And you have to -- sometimes you have to refresh. So if you just refresh your screen, it will pull up the next exhibit. It will be Exhibit 2. Just let me know when you have it.

A. All right. That's the one that says 0002?

Q. Yes, sir.

Q. The definition you have for your election system, is the only thing that's different today is that in lieu of the DRE voting machines used for casting ballots, you now have the BMDs? Was there anything --

A. So what's under those systems, like the air gap system for building ballots, it's a totally different air gap environment for building ballots, running a different application than this point. But we still have an air gap system for building ballots today. It's just got a different application inside of it.

Q. Understood.

A. The voter information page is the same, the election night reporting page is the same. Like you said, the DRE is replaced -- replaced with a different system. And all those fall under the election system umbrella.

Q. And when you say election system includes numerous other components, what are those other components?

A. Those could be networked environments, the securities applications that protect it, things like that.

Q. What networked environments are

included in the election system today?

A. So they -- at the data center where the election system is held there is a whole network environments which components for security and basically segmenting networks, the actual environment itself. Each of our environments have those kind of components in it. They're not necessarily the same. They're different based on the system that it's protecting and the system it's supporting.

Q. Anything else, any other components?

A. I'm sure there's other more detailed -- I mean, depending on how granular we want to get into defining what an environment is holding. But those are the high level things.

Q. Okay. What interactions are there, if any, between the Dominion air gaps election system that you talked about earlier that you said is air gapped and the voter registration database or E-Net?

A. Well, there is not necessarily interaction between the two. There is a data transfer that happens for each election where somebody from the election center will download a file from E-Net, it will go through numerous

on that drive that they didn't know about, we don't trust it. We clean it.

Q. Are ballot definition files stored on the state EMS for each election?

A. On the state EMS? What do you mean?

Q. The state EMS server, are ballot definition files uploaded to that server each year or for each election?

MR. DENTON: Objection.

A. I don't know the term EMS.

Q. Election management system, the Dominion -- the state server that we're talking about.

A. Oh, the ballot building system.

Q. Yes. Yes. They're -- let's just back up, make sure we're talking about the same thing. What we've been talking about is a server that the state uses that has the Dominion software on it to run elections, right?

A. Yes, that's the ballot building system.

Q. Okay.

A. So when you say EMS, now I understand what you're saying.

Q. Right.

And have you heard the term election

nobody's ever seen or proved existed, but if it did exist, did we put steps in place to make sure that malware couldn't jump on the new Android-based system? The question is why would you ask that question? Since we -- everyone knows malware that's targeted at a Windows-based access program is inert in an access database. Once again, we have to follow the two tenets of programming is the laws of physics and programming logic.

Q. Mr. Beaver, let me -- I'm going to have to help you out here, okay? You have to ask the questions I -- you have to answer the questions I ask and only what I'm asking. I'm going to get all of my questions in no matter what. We can do ten hours a day, we can do 12 hours, we can break it up into multiple days, but it's going to happen. And if you continue to give these speeches, then we'll just -- we'll either call the court and let the judge explain to you how this works or we'll just go for many, many days.

So I'm going to ask you again. I'm asking you simple yes or no questions, okay? My question is simply this: Do I understand correctly that you're not aware of any

investigation done by the state to determine whether flash drives or desktops or laptop computers or iPads, any equipment used at the county level with the old election system that would include the DREs, their GEMS servers, their poll pads, whatever -- we don't have poll pads. The GEMS servers and -- and the DREs and their elections, there's no investigation you're aware of by the state to ensure that every county replaced all of that equipment when transitioning to the Dominion system; is that true, yes or no?

MR. DENTON: Objection.

Q. You can answer.

Is it true, yes or no?

A. My understanding is a notice was sent out to the counties that they should not reuse the equipment. I do not know whether or not the counties bought all new equipment or not.

Q. Okay. Thank you.

Oh, I'm sorry, I should have asked from the start. And I'm not suggesting you are. Since we're on an online forum both sides ask these questions.

Do you have anything open other than the Zoom and the exhibit share on your computer,

Basically the industry cut their teeth on security with HIPAA, specifically targeted at medical records. So I have a number of years, over ten years, experience in programming in that environment.

Q. So my question was have you consulted any election security experts on the understanding of your software about malware?

MR. DENTON: Objection.

A. Now, I -- I don't know election security, that specific title. Anybody of that -- with that title.

Q. So, for example, Fortalice is a company that you guys rely on for -- to help with securing the election system; is that fair?

A. Yes.

Q. Did you discuss with Fortalice the view that malware potentially could be embedded in the old GEMS system, that it would be inert in the Dominion system?

A. No.

Q. Did you discuss that with the state's expert, Dr. Juan Gilbert?

A. Ron Gilbert? I don't know Ron Gilbert.

Q. Juan Gilbert, J-U-A-N.

A. I don't know Juan Gilbert.
Q. Okay. All right. Come back to Exhibit 1, if you would, please, and back to topic 1A.
A. Do you do that by going back and reopening it or is there a --
Q. Yeah. Yeah, I think -- if you closed it, you'll have to go back and reopen it.
A. Okay.
Q. And just let me know you've got that up.
A. 1A. I'm there.
Q. Okay. So just so we're clear, it's my understanding that, to your knowledge, representing the state on this topic, there is no evidence of any malware infecting the components of Georgia's current election system; is that right?
A. Correct.
Q. And what investigation was undertaken to get to that conclusion?
A. Of the current system or the old system are you asking?
Q. The current system.
A. So when we built out the system, we

built it out, as I said, as a clean system. We did not use anything that was tied to the Internet where malware can come into it, get in, infect it. We have only entered the information that has been scanned for malware into that environment.

Q. So no one, to your knowledge, has actually gone in and done any kind of forensic analysis of any of the BMDs or the Dominion servers at the state or county level to see if they are infected with malware; is that right?

A. I'm not aware of that.

Q. Do you know why that has not been done even on a sampling basis, for example?

A. Not aware that there's any sign that there is any malware on it. That's usually the first trigger to look for malware. That would be it.

Q. Well, you understand malware can successfully operate in the background without giving an indication that it's there, right?

MR. DENTON: Objection.

A. Yes, I do. But then I follow back to the tenet we talked earlier is that malware has to somehow physically get onto that environment

and have programming logic that is compatible with the environment that it's in.

Q. Right.

And I understand that, Mr. Beaver.

A. Okay.

Q. But -- okay. I get it. Thank you.

All right. Take a look at topic 1 B, please. Just let me know when you're there.

A. Yes. Yes, I'm there.

Q. This is any efforts made to air gap a components of Georgia's current election system and the success or failure of any such efforts.

A. The answer -- the answer is yes.

Q. Right.

And so what are those efforts?

A. So Secretary of State's IT group, department built an air gapped environment based on NIST standards using NIST protocols to hold the Dominion ballot building environment. And continues to maintain that air gapped environment per the NIST protocols.

Q. And that was built sometime in 20- --

A. '19.

Q. Oh, 2019?

A. I think it was -- yes.

Q. All right. And this was what you were talking about earlier that it's all new equipment, even new wires in the wall?

A. Yes.

Q. Okay.

A. It does not share anything with any other network environment. It does not cohabitate in any racks or environment.

Q. Right.

But it does share data with the voter registration system, though, right?

A. Yes. And that data is transferred using the NIST protocol.

Q. Okay. Who at the Secretary's office is actually responsible for transferring that data?

A. That would be Michael Barnes's group.

Q. Okay. Who is responsible for uploading any data or files to the state EMS server for any given election?

Is there anyone on your team that does that or is that also Mr. Barnes's group?

A. That's Mr. Barnes.

Q. Okay. All right. Take a look at topic 1 C, please.

A. Okay.

Q. And here it is any connections of any components of Georgia's current election system to the Internet, telephone lines, cable lines, satellites or other third-party system or network.

Do you see that?

A. Yes.

Q. And do you -- what connections in that topic are you aware of today?

A. So when -- when we say the election system, remember that's numerous environments. So are we talking about the Dominion air gapped environment or are we talking about the voter registration system or one of the other systems?

Q. So I -- I would use the definition that was in your -- well, strike that. Because I want to be fair.

We have a particular system -- we have a particular definition here, right? So if you come to the first page of the topics.

A. Is that going up or down? Am I scrolling --

Q. Yeah, going up. Go up back to the top. There's topic 1. Do you see that? And here you do you see at the bottom the definition of

component?

A. Oh, hold on.

Q. It's for the --

A. Component list limited to the following equipment for election...

So this all looks like it's speaking to the current Dominion environment, meaning the ballot building device --

Q. Yes.

A. -- environment.

Q. Yes, that's right.

A. It doesn't speak to any of the voter registration system, the my voter page, the online registration page. It's just the Dominion environment.

Q. Correct. Yeah.

A. Okay.

Q. And so let's --

A. So now --

Q. Yeah, let's start with that. So take a look at -- with that definition in mind, are you aware of any connections to the Internet, telephone lines, cable lines, satellites or other third-party system or network for any of the components identified in footnote two for the

scanners used to scan ballots, servings -- servers containing election management system --

A. So you're talking about the actual equipment that's in the field?

Q. Correct. That's part of it. Yeah. And so you don't -- so you don't know as you sit here whether any of the 159 counties in Georgia has ever connected any of that equipment to the Internet or to a third-party system, right?

A. No. I mean, there's some of the stuff that can't be connected, like the BMDs don't have a network connection to go into that. Now, a laptop, I'm not sure what a laptop -- what they would use a laptop for, a desktop computer, not sure how that would be involved in this whole environment. So I can't speak to those things. Smart phones, same thing, like I -- it's -- it's listed in this list, but it isn't necessarily used in the Dominion environment.

So this is a very large list of things, but not all of them have anything to do with the Dominion environment. But I can't speak to, you know, what the counties have done with these kinds of things.

Q. All right. The Dominion BMDs used in Georgia have a standard USB port on them, right?
A. Yes.
Q. In fact, the detached printer that prints the ballot connects to the BMDs with standard USB port, right?
A. Yes.
Q. And are you aware that the Dominion BMD USB ports are not sealed, meaning that a voter, for example, has access to plug in a USB drive to a BMD used in an election?
A. I don't believe that's true. It was a term it's sealed. It's not sealed. I have never seen an environment where it's not sealed. So I'm not sure where that comes from. So I guess I can't answer that that would be true. I am not aware that that -- that system is not sealed.
Q. So what is the basis for your understanding that the USB port on each of the 30,000 BMDs in Georgia is sealed?
A. I've seen them and they're sealed. And that is our protocol is to keep it sealed.
Q. Well, I assume you haven't seen all 30,000 BMDs, right?
A. No, I -- yeah, I haven't seen 30,000

BMDs. But, as I said, the protocol is to keep them sealed. And when I say sealed, they're locked -- locked away. They have a sealing device that will show tampering if somebody unseals it. So I have not heard of any counties that have had an issue with BMDs being unsealed. I have not heard that.

Q. Okay. And is that something you would expect to know as the state CIO?

A. I would have heard it. It isn't the counties report to me. You could probably ask Mr. Michael Barnes if he's heard it. I think he's more in touch with the counties than I am.

Q. And why is sealing the BMDs important?

A. Many type of layers of security. Security is not just one thing. It is a layer approach. Sealing the BMD is just one of the many security aspects to that -- verifying that we have a very secure system. Sealing is a piece of it.

Q. But what is the sealing of a BMD intended to protect against?

A. Just what you described, somebody having access to do something to it that's unknown.

coming, when they're doing the assessment to basically try to catch us off guard. Then they come back and essentially give us a results of what they they've discovered, things that they found that -- that we should look at.

Q. Okay. And do I understand right, beginning in the last couple years they're now directed to convey that orally in a conference meeting as opposed to in writing?

A. Yes.

Q. Okay. Fortalice in addition to the cybersecurity assessment, the annual assessment, Fortalice has been tasked with doing other sort of narrower, more discrete assessments from time to time for the Secretary's office; is that right?

A. Yes, it is.

Q. And when it does that, one of the requirements the Secretary's office typically has is to require monthly reporting from Fortalice on that work; is that right?

A. It has in the past, yes.

Q. But those monthly --

A. We haven't done any of that type of activity probably in the last year and a half.

Q. Why not?
A. We didn't have any events or incidents that required it.
Q. The monthly reporting, is that typically in writing or is that also now not in writing?
A. Not in writing. And in the -- we're not necessarily having any monthly reporting for a while, probably for almost the last year.
Q. So Fortalice did an annual cybersecurity assessment of CES in 2020; is that right?
A. Yes.
Q. And the findings that came out of that, those were conveyed in -- in a conference meeting with your team and others; is that right?
A. Yes.
Q. What -- what exactly was the scope of work that Fortalice did for that assessment in 2020?
A. Okay. I was not in that meeting. So I can't tell you. I don't know.
Q. Who would you ask?
A. I know Bill Warwick was involved. But he no longer works here. I forget who else?

Fortalice has not been able to penetrate the networks. We've had to let them in in order for them to continue their testing.

Q. So you anticipate where I was going to go. The 2020 and 2021 assessments included penetration testing, right?

A. Yes.

Q. And do I understand correctly, it's your understanding that the penetration testing by Fortalice failed in both 2020 and 2021?

A. My understanding is that it failed.

Q. Okay. All right. What --

A. When you say penetration testing, that means them trying to get access into our system.

Q. And what systems were they -- strike that.

You may not know because I think you said you didn't know the scope. But let me just be sure. What specific systems at the Secretary's office were within the scope of the penetration testing in 2020?

A. The only one that they could actually do potentially penetration testing is our data centers where the voter registration system is, the SOS, other applications such as corporations,

POB, securities applications are in -- e-mail environment, those. Has not -- they can't do penetrations testing on any of the CES environment, the -- a Dominion environment.

Q. Why not?

A. It is not tied to any network, whether it be Wi-Fi or hard wire that they could come through. It is completely isolated out.

Q. Have you had them test that?

A. We had them -- I think -- when we first built it, I believe that was one of the tests. But I'd have to go validate that to see whether or not there was a connection out.

Q. Okay. So as you sit here today, you don't recall any specific test Fortalice has done to penetrate the CES network; is that right?

MR. DENTON: Objection.

A. I don't know.

Q. Okay. All right. Come to paragraph 13 of your 2019 declaration, if you would. Exhibit 2.

MR. DENTON: Sorry, David, is this Exhibit 2 or 3?

MR. CROSS: Oh, good question. Maybe it's Exhibit 3. Let's see.

that also the same process today with Dominion and the poll pad software that's used?

A. That would be a Michael Barnes conversation.

Q. Okay. Is it your belief that logic and accuracy testing done on BMDs provide cybersecurity assessments for those machines?

A. It is one of the layers we use. Remember I said that security is not one thing, it's one of many layers. It's an important to valid validate that the software that's on there is what you expect to be on there and there's nothing else on that system. So yes, it is one of the layers.

Q. And is it your understanding that logic and accuracy testing actually validates the software that's on a given BMD?

A. It validates that it matches a hash test. Means if you hash the file, you will get a respondent hash. If you hash a file that has been modified at all or is of a different structure, meaning something hiding there with the same name, it will come back a different hash. And it will fail.

Q. But do you understand that it's common

with malware to design malware so that it defeats the hash test, meaning it will spit back the same hash that you're looking for when you're doing something like logic and accuracy testing?

MR. DENTON: Objection.

A. I don't have any -- any document that says that.

Q. That's not something you've heard before?

A. Nope.

Q. Okay. All right. Take a look at paragraph 18, please.

Do you have that in front of you?

A. Yes, I do.

Q. And here you wrote, State defendants also conducted parallel testing on election day for a copy of an actual county GEMS database is used with a voting machine set up in the Secretary of State's office and set an election mode for a specific real county precinct.

Do you see that?

A. Yes.

Q. Is that same sort of parallel testing done today with the Dominion system?

A. I'm not aware of that.

A. Yes.

Q. Do you have an understanding as to whether the Dominion BMD system is software independent?

A. I'm not sure I understand your question. It's software independent.

Q. Sorry. The question is just that do you have -- do you have any understanding as to whether the Dominion BMD system used in Georgia, whether it's considered software independent?

MR. DENTON: Objection.

A. I've never heard that term.

Q. Okay. Where she goes on to say that the system must be auditable and its tabulation record cannot be based solely on its software, do you have an understanding of whether the tabulation record in Georgia with the DM -- the BMD system is based on the software?

MR. DENTON: Objection.

A. I can tell you there's no voting on a BMD system. All you're doing is marking a ballot. So if somebody says you are maliciously changing votes, there are no votes counted on a BMD. So I am -- you know, I can only speculate here. But the whole conversation is sideways.

Because we don't count ballots on BMDs. It's counted over on the scanner, which runs different software completely than what's on the BMD.

Q. All right. The software on the scanner tabulates a QR code on the ballot in the current system, right?

A. I believe that's correct.

Q. And are you aware of any research or testing of the Dominion BMD system by any election security experts who found that the QR code can be changed so that it doesn't actually match what the voter intended when they voted on the BMD?

A. No, I'm not.

Q. Is that -- assuming that were a vulnerability with this system, that that could -- that that were doable, is that -- or that was a finding that was reached, is that something you would expect to know?

A. I don't know. No, apparently not. If it was a finding and I don't know.

Q. Okay. Would you expect measures to be taken to mitigate any vulnerability like that?

MR. DENTON: Objection.

A. I'd -- I'd have to know more about it.

that would be the -- the problem we had with the MVP page where you could increment the number and see other peoples' documents that they had pulled, you know, up until a point that the server clears cache.

Q. And was this -- sorry. Was this remediated?

A. As far as I know, it was remediated fairly quickly because we explained to them how to fix it.

Q. And what's the basis for your understanding that it was remediated?

A. It seems to me I had a conversation with Dave afterwards that he had worked with them to -- to understand -- you know, explain to them what it was to fix. I think they actually pulled the page down until they could fix it.

(Exhibit 16: E-mail string with the top from Chris Harvey dated 12/30/2020 marked for identification, as of this date.)

Q. Okay. All right. Grab Exhibit 16, please.

A. Chris Harvey, voter registration certificate.

Q. Yes.

So this is an e-mail you can see that Chris Harvey received on December 30th, 2020.

Do you see that from Ryan Germany?

A. Yes, yes.

Q. And if you come down the beginning of the thread it begins with an e-mail that Dave Hamilton sent on December 24, 2020.

Do you see that?

A. Yes.

Q. And he sends that to you and Mr. Germany at the Secretary's office, right?

A. Okay.

Q. And the subject line is 2020 rule 590-8-3 attestation and assessment.

Do you see that?

A. Yes.

Q. And this concerns the assessment attestation or certification that the Secretary's office has to put out each year, it's a security risk assessment that the Secretary has to attest to each year, right?

A. Yes.

Q. And so Mr. Hamilton looks like was handling the attestation in December of 2020.

Do you recall that?

A. I know it gets done every year, so -- and it needs to be the done the first -- by the end of the year or at least before -- you know, early on. I think the target is by the end of December.

Q. Okay. So do you see here --

A. I vaguely remember this.

Q. Okay. You see Mr. Hamilton writes Civix just got me the last two artifacts for this; do you see that?

A. Yes.

Q. What is Civix?

A. Civix is PCC. PCC changed their name to Civix.

Q. Okay. And he goes on, They apparently have never completed a security risk assessment. Do you see that?

A. Yes.

Q. And do you have any reason to believe that Mr. Hamilton was wrong about whether Civix or PCC had ever completed a security risk assessment?

MR. DENTON: Objection.

A. I can't speak to that.

Q. Okay.

MR. DENTON: Objection.

A. -- Dave was a -- I'll say a perfectionist. He was very judgmental of other people. And if they didn't do things his way, he wasn't satisfied. There are lots of people in the securities world. Dave was a very hard-core and that he had his vision of how things should be done. Not that his was the only way to do something, but he had his way and he spoke his mind. Here he is speaking his mind. Whether or not James actually met the level of the law, I felt he did.

Now, did Dave have a harder view on things and drive the organization better? Yeah, he did. That's why he essentially replaced James. But James did what he was supposed to do. He worked within the legal law of what requirements were. Dave was unhappy with Civix because he -- his view on security was one thing and they had a different. Security is a broad topic. Dave was very opinionated and he basically would voice his opinion all the time. So you're reading it.

Q. And the concern that Dave Hamilton expresses in this e-mail thread is that the --

the Secretary of State is actually not in compliance with the rule at this time because he can't find the evidence, what he calls artifacts, of that compliance, right?

MR. DENTON: Objection.

A. Yeah. He doesn't say here what the artifacts are. I know he and I have talked about this on multiple occasions. As I said, he was a perfectionist. The attestation applies only, only to the voting -- voter registration system, the election system. Dave felt it should apply to all things that the Secretary of State managed. But the attestation specifically only applied to election. So Dave was always on a -- on a course to say we should have things like artifacts that cover everything, whether it's the corporate registration system, whether it is the security system, professional licensing system. He felt all of them should fall under the same level of security that elections did. But the attestation clearly does not include anything but elections. And that was always a rub to Dave.

Does that answer your question?

Q. I think so. I was going to grab another exhibit for you.

A. Oh, all right I didn't -- one of those pregnant pause moments --

Q. Yes. Sorry.

(Exhibit 17: E-mail string with the top from Dave Hamilton dated 12/21/2020 marked for identification, as of this date.)

Q. All right. Grab Exhibit 17.

A. This looks like it's the same topic.

Q. Yes, yes, a little bit earlier. So I wanted to -- a little more context.

So if you go to the top, you'll see this is an e-mail that Dave Hamilton sent you on December 21, 2020 regarding the rule 590 -- or the 590 rule attestation, right?

A. Okay.

Q. If you come down in the earliest e-mail of the thread is an e-mail that Mr. Hamilton sends to you December 19, 2020 and he copies itsecurity@sos.ga.gov.

Do you see that?

A. Yes.

Q. What is the IT security e-mail there? Is that some sort of like team or group distribution list?

A. It's just an e-mail box that if we

A. Yes. But he's saying we can go from 66 up to over 80 quickly. I don't know whether he's talking about the context of Civix in like -- like we talked earlier, fixing their code so that they can't do sequel injection and things like that so we don't have to use external tools to remediate, that could very well be where he is. Because that was also a big thing is he wanted them to fix their code so it was a true fix, not a remediation using a different solution. That could very well be where he's talking. And if you notice this date timeline is all around that same time frame.

Q. Okay. But do you understand that the concern he was expressing was that with respect to what PCC was handling, the state was only in compliance with 66 percent of the requirements under the rule based on --

MR. DENTON: Objection.

Q. -- research he had done?

A. I see that. As I said, Civix code did not meet some of the requirements that we had to have from security inspection. So we had to put things in front of it to reach the level of security we needed. He was a truest. He wanted

the code to do it on its own.

So we've already talked about this topic of Civix couldn't fix their code to do what it is because it would break it. And they would have to do a major rewrite to do what really needed to do to fix the sequel injection, the cross-side scripting, those kind of things.

Q. Okay.

A. They didn't like the fact that we had to use other tools like Cloudflare to fix problems to meet our attestation levels. He wanted to see them -- like he said, we could quickly get there if Civix would just fix this. We knew that. But we couldn't -- we -- get them to fix it.

Q. All right.

A. It was a point of frustration for him.

Q. The Secretary's office has announced that they're actually moving away from E-Net, right?

A. Yes.

Q. And why is that?

A. It's an old system, to start with. Civix has changed vendors -- or has been purchased I think at least twice, maybe three

times in the last four years, four or five years.

Q. When was the decision made to move away from E-Net?

A. Last year.

Q. Who made that decision?

A. Front office.

Q. And by front office who do you mean?

A. Secretary.

Q. Oh, Secretary Raffensperger?

A. Yes. Those kind of decisions, it comes down to him to make the call. We present proposals and it's up to him to say yay, nay.

Q. What --

A. It's a big decision.

Q. Sorry.

A. Yeah, that was a big, big decision.

Q. What were those specific reasons that he decided to move -- to replace E-Net?

A. One was the age, one was the ability for us to get, like this, certain fixes put in place that we wanted to see. Some of it was security related, some was just functionality related. The application was built I think like in 2012 when we first purchased it. And the -- but the actual application was probably built a

year or two before that. So the core code was ten years old. Getting very old. Technology has changed. So it was time to look at another solution. We were in the process of also looking at some of our other systems and we decided to do basically an overall refit of everything.

Q. What's the new solution that you're bringing in in place of E-Net?

A. I think they've announced -- already announced that it's Salesforce based.

Q. And will that be a cloud solution hosted by Salesforce?

A. Yes.

Q. Okay. What's the process for migrating data from E-Net to Salesforce; do you know?

A. It hasn't been done yet. We're in the process of trying to come up with a migration plan.

(Exhibit 18: 2020 Security of the voter registration system artifacts and attestation pursuant to Rule 590-8-3-.01 December 18, 2020 marked for identification, as of this date.)

Q. All right. Grab Exhibit 18, please.

A. 2020 security of voter registration

whole technology team.

Q. All right. Can you come back, if you would, please, to Exhibit 19, which was the cover e-mail for the remediation task list.

A. Got it.

Q. And so in Mr. Hamilton's e-mail to you he writes, How much do we want to share of this? Normally how we prioritize and what we are working on is not ever meant for public eyes. And then he goes on to say, This level of detail I don't think we should give anyone outside the agency because it can be used to pinpoint where our holes are and give a road map to bad actors.

Do you see that?

A. Yep.

Q. Did you share his concern that if you were going to make public the attachment that it could be used to pinpoint where holes were in the Secretary's network and give a road map to bad actors?

A. I think anytime you reveal any security information about an organization, you give a road map to bad actors. That is -- that is like the number one thing that bad actors look for is any public information about how a system's

designed, known information about it. That's why bad actors typically scan sites all the time looking for holes. So anytime you give them something, that's not good. You're just basically making it even more difficult on yourself to protect your system.

Q. If you can pull up Exhibit 20 again.

A. Yes.

Q. Are there any specific risks in here that you can identify as an example where it -- you would be concerned about making them public because of the road map concern?

A. I don't know that I can answer that. I -- any risk -- this is what you hear in the paper all the time that, you know, Adobe has no risk. Well, more than likely nobody knows about it but maybe a researcher someplace. But as soon as you open it up, now people can say oh, let me go look over there. I mean, the Internet is a wide field. As soon as you start to point to well, here is a potential area, it let's people focus on that and you would become more exposed.

That doesn't mean that the risk it -- probability of somebody actually penetrating it is very high at all. Because somebody still has

to find that needle out in that field. But if someone says it's right there, you make it much easier. Not necessarily they can penetrate or breach you, but it gives them a target.

So I wouldn't speak of any of these over another because each one of them are -- are risks that need to be looked at. Now, what's the probability that somebody will find them? Hopefully very low. Probably very low considering we've never had a breach. The -- we're running pretty good. But Dave's job was to find all of those pins in the field. And he was -- he was relentless. That's why he was good. My stand on security people is if they're not a total pain in your ass, they're not doing their job.

Q. Who has Dave Hamilton's responsibilities now as the CISO?

A. So it's tied between Kevin Fitts and Fortalice. Dave is hard to replace.

Q. How long has Kevin Fitts been with your office?

A. About eight years.

Q. And he reports to you?

A. Yes.

Q. And what responsibilities does Fortalice have for filling in part of the CISO role?

A. So the key strategic where do we go, what are the core elements that we need to work on, Kevin Fitts does not have that level of experience of a CISO. He is not a CISO. He's a manager, he's certified in security. But he doesn't have the years of experience Dave had. So until we figure out how to replace Dave, Kevin is helping me fill in the position of helping to manage the day-to-day.

I mean, so for like risk registers, once it's been identified where the issues are, we need to start working -- working a plan on each of these. And each of these could take months to fix. And some of them that are what are considered high risk maybe probability is someone actually attacking it is really low. But if they were to find it, it would cause a problem.

So his task is working with Fortalice to identify all right, let's work on these five things first. Because you can only do so much at a time. It's a working environment. This is not

Q. Okay.

A. The important thing here is we track what our weaknesses are and we work toward fixing them. Too many organizations that I've seen do turn a blind eye to try to keep track of this. This is what's made our organization strong security-wise is we keep track of it, we hold ourselves accountable.

Q. And sorry, Mr. Beaver, if I asked you this earlier, but I can't remember. We talked about, you know, possible forensic examination of voting equipment like BMDs and printers and scanners. Do you know why that has not been done in Georgia?

MR. DENTON: Objection.

A. No. I have not been involved in a question about doing that. So I don't have -- I couldn't answer you either way.

Q. So that's not something you've proposed as the CIO; is that fair?

A. That is fair.

Q. Okay. And are you aware of any discussion or consideration at the Secretary's office about doing that or you've just not heard anything like that?

A. Correct. I have not heard anything.
Q. Okay. Who would have the authority to make the decision to do that type of analysis?
A. It would be between the election center, the elections department, Gabe Sterling and the Secretary. If an issue bubbled up that pointed to a risk, meaning it's verified that something has happened that shows that something, you know, has happened, yeah, we probably would act on it. If we get an e-mail from somebody saying I'm going to start hacking your system, beware, that's probably not enough information to jump on, oh, let's run a test on all the stuff.
Q. Okay.
A. And you've seen it.
Q. Are you familiar with something called the SolarWinds hack?
A. Yes.
Q. And do you recall that nine Georgia counties, there was evidence that they may have downloaded malware related to that hack in February of 2021?
A. I didn't know the count. I knew that there were some counties that were vulnerable.
Q. Were you involved in any investigation

servers so I could have multiple servers. And what we did was create virtual desktops for the people to use so, actually, code doesn't transfer over the network to that PC that's on their desktop. They use a browser window into a virtual desktop that sits on the server. It's just the configuration we did.

Q. How are the PCs that access the EMS server -- what is the -- what are the mechanics of connecting to that server?

A. It's an Ethernet hard-wired cable.

Q. And so when people are working on those PCs, are they sitting in a room physically with the server or where are they sitting?

A. No. In their desks. That's why we had to run new wires in the wall.

Q. Oh, I see. So the people who have access to the EMS server, they work from their offices on a PC that's hard-wired to the server and that server sits in some room somewhere; is that correct?

A. A caged room.

Q. Okay.

A. Elsewhere in the building.

Q. Okay.

A. So the typical configuration of the office is you have a desk on one side, you turn one way and you're working on your PC for daily e-mail and stuff and it's tied to the Internet. And you turn around and you face the opposite direction and you're working on PC that's on the air gap network.

Q. Got it.

Okay. And so I may have said this before. How many people have those PCs in their offices? Just approximately.

A. Oh, five, maybe eight. It's depending on -- I think at the beginning when we had a big push we had as many as eight. But I think they're down to about five now.

Q. Okay. And then if you come to where -- see where it says supports SQL Express and Win 10, do you see that, just where we were?

A. Yes.

Q. And then below that it reads, Windows 10 running XP guest to access old system.

Do you see that?

A. Yes.

Q. Do you know what that refers to?

A. So we were still -- remember we were

running in parallel in a different environment, the old GEMS system. Because we hadn't completely switched over. So they were -- as part of the project they had to make sure that they had the machines that could run the old system, they had machines that could run the new system. The old system had to run XP because the GEMS application run -- ran with XP.

Q. All right.

A. Two totally different environments.

Q. And just so I understand, when you say two totally different environments, the Dominion EMS server you said was locked in the cage somewhere. Was the old GEMS system, whatever servers it was still running on, was that locked in a different cage somewhere?

A. It was in a different rack. A different rack. You know what a rack is?

Q. Yes, yes, yes. So it's all in the same locked cage?

A. Locked area.

Q. But it's on a different server rack?

A. Yes.

Q. Got it.

And you're saying there were no -- no

REPORTER'S CERTIFICATE

I, V. Dario Stanziola, a Certified Court Reporter in the State of Georgia, duly commissioned and authorized to administer oaths and to take and certify depositions, do hereby certify that on Wednesday, February 2, 2022, Sanford Merritt Beaver, being by me personally duly sworn to tell the truth, thereupon testified as above set forth as found in the preceding pages, this examination being recorded stenographically by me verbatim and then reduced to typewritten form by me, that the foregoing is a true and correct transcript of said proceedings to the best of my ability and understanding; that I am not related to any of the parties to this action; that I am not interested in the outcome of this case; that I am not of counsel nor in the employ of any of the parties to this action.

IN WITNESS WHEREOF, I have hereto set my hand, this the 8th day of February 2022.

_____

V. DARIO STANZIOLA, CCR (GA)(NJ), RPR, CRR
Certification Number: 4531-3928-0743-6288